



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0070158
(43) 공개일자 2012년06월29일

(51) 국제특허분류(Int. Cl.)

G06K 9/20 (2006.01)

(21) 출원번호 10-2010-0131592

(22) 출원일자 2010년12월21일

심사청구일자 2010년12월21일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

정용화

대전광역시 유성구 은구비로 31, 열매마을아파트
505동 402호 (지족동)

이성주

서울특별시 마포구 월드컵북로22길 20 (성산동)

최우용

대전광역시 유성구 엑스포로 448, 304동 1204호
(전민동, 엑스포아파트)

(74) 대리인

특허법인충현

전체 청구항 수 : 총 11 항

(54) 발명의 명칭 지문 정보 보호 시스템 및 그 방법

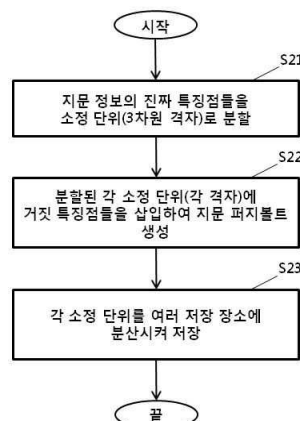
(57) 요약

본 발명은 지문 정보 보호 방법에 관한 것으로, 상관 공격(Correlation Attack)에 강인한 지문 퍼지 볼트를 구현하여 지문 정보의 보호를 꾀할 수 있는 방법에 관한 것이다.

본 명세서에서 개시하는 지문 정보 보호 방법은 (a)지문 정보의 진짜 특징점들을 소정 단위로 분할하는 단계; (b)상기 분할된 각 소정 단위에 상기 지문 정보의 거짓 특징점들을 삽입하여 상기 지문 정보의 지문 퍼지 볼트를 생성하는 단계; 및 (c)상기 각 소정 단위를 여러 저장 장소에 분산시켜 저장하는 단계를 포함하여 본 방법 발명의 과제를 해결한다.

본 발명에 의하면, 지문 정보의 진짜 특징점이 위치하는 3차원 격자의 빈 격자에 거짓 특징점을 비임의적(규칙적)으로 그리고 하나씩만 삽입하여 지문 퍼지 볼트를 생성하기 때문에 상관 공격자로 하여금 진짜 특징점과 거짓 특징점을 구별하기 매우 어렵게 하며, 아울러 격자 단위로 지문 퍼지 볼트를 여러 저장 장소에 분산 저장하기 때문에 상관 공격자로 하여금 지문 퍼지 볼트의 재구성을 매우 난해하게 하므로 지문 퍼지 볼트의 상기한 생성 방식과 결합하여 지문 정보의 안전성 확보를 현저히 제고시킬 수 있다.

대표도 - 도2



특허청구의 범위

청구항 1

- (a)지문 정보의 진짜 특징점들을 소정 단위로 분할하는 단계;
- (b)상기 분할된 각 소정 단위에 상기 지문 정보의 거짓 특징점들을 삽입하여 상기 지문 정보의 지문 퍼지 볼트를 생성하는 단계; 및
- (c)상기 각 소정 단위를 여러 저장 장소에 분산시켜 저장하는 단계를 포함하는 지문 정보 보호 방법.

청구항 2

- 제 1 항에 있어서,
- 상기 (a)단계는 상기 진짜 특징점들을 3차원 격자들(3D lattices)로 분할하는 단계이며,
- 상기 (b)단계는 상기 거짓 특징점들을 상기 3차원 격자들의 각 격자에 삽입하여 상기 지문 퍼지 볼트를 생성하는 단계이며,
- 상기 (c)단계는 상기 각 격자를 상기 여러 저장 장소에 분산시켜 저장하는 단계인 것을 특징으로 하는 지문 정보 보호 방법.

청구항 3

- 제 2 항에 있어서, 상기 (b)단계에 의한 삽입은
- 상기 진짜 특징점들이 위치하지 아니한 격자에만 삽입하는 것으로 이루어지는 것을 특징으로 하는 지문 정보 보호 방법.

청구항 4

- 제 3 항에 있어서, 상기 (b)단계에 의한 삽입은
- 상기 각 격자에 하나의 거짓 특징점만 삽입하는 것을 특징으로 하는 지문 정보 보호 방법.

청구항 5

- 제 2 항 내지 제 4 항 중 어느 한 항에 있어서, 상기 (c)단계는
- 상기 각 격자를 임의적 순번으로 저장하거나 상기 여러 저장 장소의 각 저장 장소의 임의적 순번대로 저장하여 이루어지는 것을 특징으로 하는 지문 정보 보호 방법.

청구항 6

- 제 5 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체.

청구항 7

- 지문 정보의 진짜 특징점들을 소정 단위로 분할하는 분할부;
- 상기 분할된 각 소정 단위에 상기 지문 정보의 거짓 특징점들을 삽입하여 상기 지문 정보의 지문 퍼지 볼트를 생성하는 생성부; 및
- 상기 각 소정 단위를 여러 저장 장소에 분산시켜 저장하는 분산 저장부를 포함하는 지문 정보 보호 시스템.

청구항 8

- 제 7 항에 있어서,
- 상기 분할부는 상기 진짜 특징점들을 3차원 격자들(3D lattices)로 분할하고,
- 상기 생성부는 상기 거짓 특징점들을 상기 3차원 격자들의 각 격자에 삽입하여 상기 지문 퍼지 볼트를 생성하

며,

상기 분산 저장부는 상기 각 격자를 상기 여러 저장 장소에 분산시켜 저장하는 것을 특징으로 하는 지문 정보 보호 시스템.

청구항 9

제 8 항에 있어서, 상기 생성부는

상기 진짜 특징점들이 위치하지 아니한 격자에만 상기 거짓 특징점들을 삽입하는 것을 특징으로 하는 지문 정보 보호 시스템.

청구항 10

제 9 항에 있어서, 상기 생성부는

상기 분할된 각 격자에 하나의 거짓 특징점만 삽입하는 것을 특징으로 하는 지문 정보 보호 시스템.

청구항 11

제 8 항 내지 제 10 항 중 어느 한 항에 있어서, 상기 분산 저장부는

상기 각 격자를 임의적 순번으로 저장하거나 상기 여러 저장 장소의 각 저장 장소의 임의적 순번대로 저장하는 것을 특징으로 하는 지문 정보 보호 시스템.

명세서

기술 분야

[0001] 본 발명은 지문 정보 보호 시스템 및 그 방법에 관한 것으로, 보다 상세하게는 지문 퍼지 볼트(Fingerprint Fuzzy Vault)를 이용하여 지문 정보의 보호를 꾀하는 것이고, 특히 상관 공격(Correlation Attack)에 강인한 지문 퍼지 볼트를 구현하여 지문 정보의 보호를 꾀할 수 있는 시스템 및 그 방법에 관한 것이다.

배경 기술

[0002] 개인 정보의 하나인 지문 정보를 보호할 수 있는 여러 방안들이 연구되고 있거나 산업적으로 실시되고 있는데, 그 중 지문 퍼지 볼트를 구현하여 지문 정보를 보호하는 방안이 안전성 제고 측면 및 지문 정보의 활용이 요구되는 시스템의 부하 감소를 꾀할 수 있는 측면에서 매우 각광받고 있다.

[0003] 그러나 지문 퍼지 볼트를 매우 쉽게 크래킹(cracking)할 수 있는 상관 공격(Correlation Attack) 기법이 알려져([W. Scheirer and T. Boulton, "Cracking Fuzzy Vaults and Biometric Encryption," 2007.], [A. Kholmatov and B. Yanikoglu, "Realization of Correlation Attack against the Fuzzy Vault Scheme," Proc. of SPIE, 2008.]), 지문 퍼지 볼트를 이용한 지문 정보 보호 방안은 특히 안전성 확보 측면에서 취약한 보호 방안으로 간주되기에 이르렀다.

[0004] 지문 퍼지 볼트에 대한 상관 공격 기법은 동일한 지문으로부터 생성되는 두 개의 지문 템플릿(template)을 획득하여 지문 정보의 진짜 특징점(real minutiae)과 거짓 특징점(chaff minutiae)을 매우 쉽게 구별해 낸다. 아울러 상관 공격 기법은 지문 퍼지 볼트에만이 아니라, 지문 퍼지 볼트처럼 진짜 특징 정보의 기밀성을 제공하기 위해 거짓 특징 정보를 임의로 삽입하는 모든 암호화 방식을 공격할 수 있는 기법이다. 즉, 지문 퍼지 볼트에 직접 적용 가능한 공격 기법이기에 때문에 이를 방지하는 방안이 반드시 필요하다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 상기한 필요성에 부응하기 위해 창안된 것으로, 본 발명이 해결하려는 과제는 상관 공격에 강인한 지문 퍼지 볼트를 구현하여 지문 정보의 보호를 꾀할 수 있는 방안을 제시하는 것이다.

과제의 해결 수단

[0006] 상기과 같은 과제를 해결하기 위해 본 명세서에서 개시하는 지문 정보 보호 방법은

[0007] (a)지문 정보의 진짜 특징점들을 소정 단위로 분할하는 단계; (b)상기 분할된 각 소정 단위에 상기 지문 정보의 거짓 특징점들을 삽입하여 상기 지문 정보의 지문 퍼지 볼트를 생성하는 단계; 및 (c)상기 각 소정 단위를 여러 저장 장소에 분산시켜 저장하는 단계를 포함하여 본 방법 발명의 과제를 해결한다.

[0008] 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 지문 정보 보호 시스템은

[0009] 지문 정보의 진짜 특징점들을 소정 단위로 분할하는 분할부; 상기 분할된 각 소정 단위에 상기 지문 정보의 거짓 특징점들을 삽입하여 상기 지문 정보의 지문 퍼지 볼트를 생성하는 생성부; 및 상기 각 소정 단위를 여러 저장 장소에 분산시켜 저장하는 분산 저장부를 포함하여 본 시스템 발명의 과제를 해결한다.

발명의 효과

[0010] 본 발명에 의하면, 거짓 특징점을 지문 정보의 진짜 특징점이 위치하는 3차원 격자들 중 빈 격자에만 비임의 적(규칙적)으로 그리고 하나씩만 삽입하여 지문 퍼지 볼트를 생성하기 때문에 상관 공격자로 하여금 진짜 특징점과 거짓 특징점을 구별하기 매우 난해하게 한다.

[0011] 이와 더불어 지문 퍼지 볼트가 구현된 3차원 격자들의 각 격자를 여러 저장 장소에 분산 저장하기 때문에 상관 공격자로 하여금 지문 퍼지 볼트의 재구성을 매우 난해하게 하므로 지문 퍼지 볼트의 상기한 생성 방식과 결합하여 지문 정보의 안전성 확보를 보다 더 제고시킬 수 있다.

도면의 간단한 설명

[0012] 도 1은 본 시스템 발명의 바람직한 일 구성을 제시한 도면이다.

도 2는 본 방법 발명의 바람직한 일 흐름을 제시한 도면이다.

도 3은 본 발명에 의해 생성되는 지문 정보의 일례를 제시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 발명을 실시하기 위한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하려는 과제의 해결 방안의 개요를 우선 제시한다.

[0014] 본 발명은 상관 공격에 강인한 지문 퍼지 볼트를 생성하여 지문 정보의 보호를 피함에 있어서, 지문 퍼지 볼트를 소정 단위로 분할하고 분할된 각 소정 단위를 여러 저장 장소에 분산시켜 저장하는 것으로 상관 공격에 의한 지문 정보의 부당한 유출을 방지한다. 지문 퍼지 볼트를 소정 단위로 분할하여 여러 곳에 분산시켜 저장시키면, 지문 정보 인증시에 분산 저장된 지문 퍼지 볼트를 결합하여 완성된 형태의 퍼지 볼트로 재구성하는 작업이 매우 난해해지므로 상관 공격에 강인해지는 것이다.

[0015] 이하, 본 발명을 실시하기 위한 구체적인 내용을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0016] 도 1은 본 시스템 발명의 바람직한 일 구성을 제시한 도면이며, 도 2는 본 방법 발명의 바람직한 일 흐름을 제시한 도면이다.

[0017] 분할부(11)는 지문 정보의 진짜 특징점들을 소정 단위로 분할한다(S21). 지문 정보는 예를 들어 지문이 포함된 영상에서 지문 특징점들(진짜 특징점들)의 2차원 평면상에서의 위치(X, Y) 및 각도를 포함하여 구성되는 지문 정보를 추출하는 것으로 획득될 수 있다.

[0018] 한편 분할부(11)에 의한 진짜 특징점의 소정 단위로의 분할은 진짜 특징점들을 3차원 격자들(3D lattices)로 분할로 분할하는 것이 바람직하다. 3차원 격자들로 분할하기 위해서는 진짜 특징점의 정보를 3차원으로 표현함이 필요한데, 진짜 특징점들의 평면상에서의 위치(X, Y) 및 각도 중 각도를 Z축 좌표로 변환하여 진짜 특징점의 정보를 (X, Y, Z)의 3차원 정보로 표현한다. 각도의 Z축 좌표로의 변환은 예를 들어 다음과 같이 이루어진다.

$$Z_i = \frac{\theta_i}{360} \times M_z$$

- [0019]
- [0020] 여기서, θ_i 는 i 번째 진짜 특징점(각 진짜 특징점)의 각도이고, Z_i 는 i 번째 지문 특징점의 각도가 변환된 i 번째 지문 특징점에 대한 Z 축 좌표 값이며, M_z 는 설정된 최대 Z 축 좌표값이다.
- [0021] 생성부(12)는 분할된 각 소정 단위에 지문 정보의 거짓 특징점들을 삽입하여 지문 정보의 지문 퍼지 볼트를 생성한다(S22). 여기서 각 소정 단위란 3차원 격자들의 각 격자를 의미하는 것으로, 생성부(12)는 각 격자에 거짓 특징점들을 삽입하여 지문 퍼지 볼트를 생성하는데, 거짓 특징점들의 삽입은 다음과 같이 이루어질 수 있다.
- [0022] 생성부(12)는 거짓 특징점들을 각 격자에 '규칙적'으로 삽입한다. 여기서 '규칙적'으로 삽입한다는 의미는 3차원 격자들 중 진짜 특징점이 위치하지 않는 격자에만 거짓 특징점들을 삽입한다는 의미이다.
- [0023] 원래 지문 퍼지 볼트는 진짜 특징점에 거짓 특징점을 '임의적으로(randomly)' 삽입하여 형성되는 것이 통상적이다. 이는 거짓 특징점이 삽입되는 위치가 임의적으로 될 수 있다는 의미이다. 그러나 본 발명에서는 진짜 특징점들이 위치하지 않는 격자에만 거짓 특징점들이 삽입되는데, 진짜 특징점들이 위치하지 않는 격자에만 삽입되므로 비임의적 위치에 삽입된다는 의미이고 '규칙적 삽입'의 의미는 이러한 삽입을 의미하는 것이다.
- [0024] 생성부(12)는 아울러 거짓 특징점들을 상기와 같이 비임의적으로 삽입하되, 각 격자에 하나의 거짓 특징점만 삽입시킨다(단일 삽입). 생성부(12)에 의해 생성된 지문 퍼지 볼트의 예가 도 3에 제시되어 있는데, 지문 퍼지 볼트는 하나의 지문 정보에서 여러 개가 생성이 가능하며 도 3에는 두 개의 예((a)와 (b))를 제시한 것이다.
- [0025] 한편 상기한 비임의적 삽입과 단일 삽입으로 인해 상관 공격에 강인해질 수 있는데, 그 이유를 제시하면 다음과 같다.
- [0026] 상관 공격의 핵심은 공격자가 두 개의 지문 퍼지 볼트(예를 들어 도 3의 (a)와 (b))를 매칭(matching)시켜 가장 많이 매칭되는 형태로부터 진짜 특징점을 추출하는 것이다. 본 발명에 의한 생성부(12)에 의해 지문 퍼지 볼트를 생성하게 되면(예를 들어 도 3과 같이), 공격자가 두 개의 지문 퍼지 볼트를 획득한다 하여도 상기와 같이 비임의적으로(규칙적으로) 그리고 각 격자에 거짓 특징점을 하나만 삽입하였기 때문에 획득한 두 개의 지문 퍼지 볼트를 매칭시켜도 다량의 거짓 특징점이 포함된 상태로 진짜 특징점이 추출된다. 이는 진짜 특징점과 가짜 특징점의 구별(distinguishment)이 용이하지 않음을 의미하는 것이고 따라서 상관 공격에 강인한 것이다.
- [0027] 분산 저장부(13)는 각 소정 단위를 여러 저장 장소에 분산시켜 저장한다(S23). 즉, 분산 저장부(13)는 지문 퍼지 볼트가 구현된 3차원 격자들의 각 격자를 여러 저장 장소에 분산시켜 저장시킨다.
- [0028] 본 발명에 의한 지문 퍼지 볼트의 생성은 상기한 바에 의해서도 즉, 거짓 특징점을 비임의적으로(규칙적으로) 그리고 각 격자에 하나만 삽입하는 것만으로도 상관 공격에 충분히 강인할 수 있다. 그러나 이 경우 만일 진짜 특징점이 매우 많은 경우에는 삽입되는 거짓 특징점이 매우 적어 진짜 특징점과 거짓 특징점의 구별이 매우 용이해질 수 있으므로 상관 공격에 쉽게 노출될 수 있는 문제가 있을 수 있다.
- [0029] 그리고 지문 퍼지 볼트를 구성하는 모든 특징점들을 한 곳의 저장 장소에만 저장시키는 경우 특히, 지문 정보 인증시에 지문 정보 전체가 하나의 저장 장소에서 일괄적으로 독출될 수 있으므로 이 또한 상관 공격을 포함한 외부로부터의 공격에 취약해질 수 있는 가능성이 높아진다.
- [0030] 따라서 본 발명에서는 상기한 지문 퍼지 볼트 생성 방식을 보완하여 보다 더 완벽한 보호를 기할 수 있는 방안을 제시하는데, 이는 분산 저장부(13)에 의해 실현된다.
- [0031] 분산 저장부(13)는, 위에서 언급한 바와 같이, 지문 퍼지 볼트가 구현된 3차원 격자들의 각 격자를 여러 저장 장소에 분산시켜 저장시킨다. 여기서 여러 저장 장소는 단일 시스템내의 논리적으로 분리된 여러 저장 장소일 수도 있고, 물리적으로 분리된 여러 저장 시스템일 수도 있다.
- [0032] 한편 분산 저장부(13)가 각 격자를 여러 저장 장소에 분산시켜 저장시에는 각 저장 장소의 순번대로 저장하는 것이 아니라 임의적 순번으로 저장시킨다. 예를 들어 여러 저장 장소가 4개이며 저장 장소 1, 저장 장소 2, 저장 장소 3, 저장 장소 4의 순번을 가지고 있고, 3차원 격자의 수가 16개가 있다고 가정하자. 분산 저장부(13)는 1번 격자는 저장 장소 1번에, 2번 격자는 저장 장소 2번에, 3번 격자는 저장 장소 3번에, 4번 격자는

저장 장소 4번에, ..., 13번 격자는 저장 장소 1번에, 14번 격자는 저장 장소 2번에, 15번 격자는 저장 장소 3번에, 16번 격자는 저장 장소 4번에 저장하는 방식이 아니라, 1번 격자는 저장 장소 4번에, 2번 격자는 저장 장소 3번에, 3번 격자는 저장 장소 1번에, ..., 13번 격자는 저장 장소 2번에, 14번 격자는 저장 장소 1번에, 15번 격자는 저장 장소 3번에 저장하는 방식으로 즉, 저장 장소의 임의적 순번으로 저장을 하는 것이다.

[0033] 이러한 임의적 순번은 비단 저장 장소에 대해서만 적용되는 것이 아니며, 격자의 저장 순번에도 적용될 수 있다. 즉, 위의 예에 의할 때 1번 격자, 2번 격자, ..., 16번 격자 순서대로 저장하는 것이 아니라, 4번 격자, 7번 격자, 13번 격자, ...의 임의적 순번으로 저장시킬 수 있다. 다만, 지문 인증 시스템의 부하, 보안 환경 등 제반 환경을 고려하여 저장 장소의 순번만을 임의로 할 것인지 격자의 저장 순서만을 임의로 할 것인지 아니면 두 순번 모두를 임의로 할 것인지 결정될 수 있다.

[0034] 지문 인증이 요구되는 경우 상기한 방식과 같이 분산 저장된 지문 퍼지 볼트를 결합시켜 완전한 형태의 지문 퍼지 볼트의 재구성이 필요한데, 상기한 분산 저장 방식으로 인해 상관 공격자에 의한 지문 퍼지 볼트의 재구성을 매우 난해하게 만든다. 즉, '분산'과 '임의적 순번'에 의한 저장으로 인해 공격자의 입장에서는 재구성 작업이 매우 난해하므로 공격의 어려움이 현저히 배가된다. 따라서 지문 퍼지 볼트의 상기한 생성 방식과 분산 저장 방식이 결합되어 지문 퍼지 볼트로 구성된 지문 정보 보호의 안전성을 보다 더 획기적으로 제고시킬 수 있다.

[0035] 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

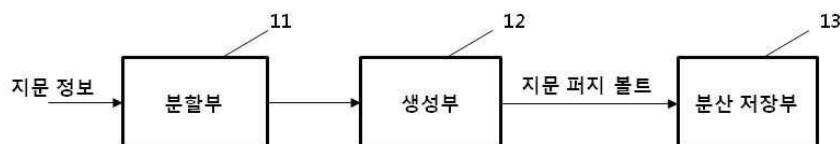
[0036] 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0037] 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다.

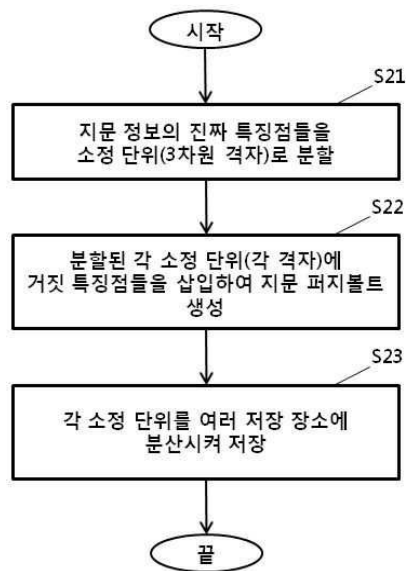
[0038] 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

도면1



도면2



도면3

